Information Assurance Awareness (v9)
Security Tips Summary

A Risk to One is a Risk to All!

Remember to:	By following these tips:
Create Secure Passwords	Do not use personal information Combine capital and lower case letters, numbers, special characters Do not use common phrases or words Do not write down your password, memorize it Change password regularly
Avoid Phishing Attempts	Do not access the web by selecting links in e-mails or pop-up messages View all e-mail in the plain text Contact the organization using a telephone number Type the web address or use bookmark Delete the e-mail
Avoid Spear Phishing Attempts	Never give out your password IT and help desk personnel will never ask for your password Never reveal any personal information in an e-mail Look for digital signatures
Forward E-mails Carefully	Use online sites to confirm or expose potential e-mail hoaxes Do not forward e-mail hoaxes
Read E-mails Carefully	View e-mail in plain text Use caution when opening e-mail All attachments should be scanned Delete e-mail from senders you do not know Turn off automatic downloading
Use E-mail Appropriately	• E-mail must not: Adversely affect performance Reflect poorly on the Government • Do not use e-mail to: Sell anything Send chain letters Send offensive letters • Do not send: Mass e-mails Jokes or Pictures Inspirational stories • Avoid using *Reply All* Personal e-mail use may be authorized
Avoid Computer Misuse	Examples of Computer Misuse: • Viewing/downloading pornography • Gambling on the Internet • Private business/money-making ventures • Loading personal/unauthorized software • Unauthorized configuration changes
Protect Against Spillage	Check all documents for classification level Know the different types of networks NIPRNet - for unclassified data SIPRNet – for classified data Be aware of which network you are on

Information Systems Security Awareness (v4)
Security Tips Summary (cont'd)

Remember to:	By following these tips:
	Label all files, removable media, and subject headers If a spillage occurs, notify your security POC When storing or transmitting sensitive information, including PII: Encrypt before storing on mobile devices or transmitting E-mail with caution Store on authorized system Never transmit, store, or process on a non-sensitive system
Avoid Social Engineering Attempts	Do not participate in telephone surveys Do not give out personal information Do not give out computer or network information Do not follow instructions from unverified personnel Document interaction: Verify the identity of all individuals Write down phone number Take detailed notes Contact your security POC
Follow Physical Security Procedures	Use your own security badge or key code Never grant access for someone else Maintain possession of your CAC at all times Challenge people Report suspicious activity
Avoid Computer Viruses	• Scan all external files before uploading to your computer • Do not e-mail an infected file to anyone • Contact your help desk for assistance
Conduct E-Commerce Cautiously	• Set your browser preferences to prompt you each time a website wants to store a cookie • Only accept cookies from reputable, trusted websites. • Confirm that site uses encrypted links (https)
Follow Home Security Tips	Turn on password feature and use strong passwords Install all system and application security updates and patches Keep anti-virus software up-to-date Regularly scan files for viruses Install spyware protection software Turn on firewall protection Require confirmation before installing mobile code Regularly back up and securely store your files
Follow FAX Procedures	• Ensure that the recipient is at the receiving end • Use the correct cover sheet • Contact the recipient to confirm receipt • Never transmit classified information via an unsecured fax machine

Information Systems Security Awareness (v4)
Security Tips Summary (cont'd)

Remember to:	By following these tips:
Follow Telework Guidelines	You may telework from a telework center You may work at home, in a dedicated work area You must use authorized equipment and software You must implement appropriate security measures You must sign a telework agreement You must sign a safety checklist You must protect your data
Follow Travel Tips	Be careful of information visible on your laptop Ensure that the wireless security features are properly configured Wireless technology is not a secure technology Never discuss sensitive information on an unsecured phone Maintain possession of your laptop at all times Password protect your laptop Encrypt all sensitive and unclassified information not cleared for public release
Protect Your Identity	• Ask how information will be used before giving it out • Pay attention to credit card and bank statements • Avoid common names/dates for passwords and PINs • Pick up mail promptly • Shred personal documents • Carry your SSN card and passport only when necessary • Order credit report annually **Responding to identity theft:** • Contact credit reporting agencies • Contact financial institutions/creditors to place an alert on: Credit cards Bank accounts • Monitor credit card statements for unauthorized purchases • Report crime to the local police

Information Systems Security Awareness (v4)
Security Tips Summary (cont'd)

Remember to:	By following these tips:
Handle Removable Media Appropriately	Examples: thumb drives, flash drives, CDs, DVDs, external hard drives • Do not use thumb drives/flash media unless operationally necessary • Do not use any personally owned/non-Government removable media on DoD systems • Do not use Government removable media on non-DoD/personal systems • Encrypt all data stored on removable media • Encrypt in accordance with the data's classification or sensitivity level • Use only removable media approved by your organization • Store in GSA approved storage containers at the appropriate level of classification • Contact your security POC for more information
Handle Mobile Computing Devices Appropriately	Examples: personal digital assistants (PDAs), laptops, cell phones, and other portable electronic devices (PEDs), wireless readers (e.g., Kindle and iPads); music players such as iPods). • Be extra vigilant when storing data on mobile computing devices • All mobile computing devices must comply with DoD policy • All DoD information on mobile computing devices must be encrypted • Encrypt all Personally Identifiable Information (PII) on mobile computing devices o Social Security Numbers o Dates and places of birth o Mothers' maiden names o Biometric records • DoD classifies laptop computers as a mobile computing device • **Never** cross classification boundaries Never unplug mobile devices from SIPRNet to connect to the NIPRNet, or vice-versa Does not matter whether or not the device's memory has been purged If lost or stolen, immediately report the loss to your security POC If the device contains PII, the loss must also be reported: • within one hour to the U.S. Computer Emergency Response Team (CERT) • within 24 hours to the Component Privacy Office • within 48 hours to the DoD Privacy Office • Encrypt all Personally Identifiable Information* (PII) on mobile computing devices Social Security Numbers Dates and places of birth Mothers' maiden names Biometric records • If lost or stolen, immediately report the loss to your security POC If the device contains PII, you must report the loss **immediately** to your organization's security POC or help desk • Contact your security POC for more information *Note: PII is Any information about an individual maintained by an agency, including, but not limited to education, financial transactions, medical history, criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, and biometric records, including any other personal information that is linked or linkable to an individual.

Information Systems Security Awareness (v4)
Security Tips Summary (cont'd)

Remember to:	By following these tips:
Follow Tips for Active X and Other Mobile Code Technology	• Require confirmation before enabling • Only allow mobile code to run from DoD or DoD trusted sites
Identify and Handle Classified Information Properly	• Assigned classification level by classification authority • Used in area with security appropriate to classification level • Stored in GSA approved vault/container
If Permitted by Agency to Access Web Mail, Use with Caution	Use caution if you are allowed to use web mail on Government computers. By using web mail, you are bypassing firewalls and other security measures, and exposing you and your agency to potential viruses and other malware.
If Permitted by Agency to Use Social Networking Sites, Follow Best Practices	Use caution if you are allowed to use social networking sites on Government computers. Best practices include: • Consider carefully the information you post online about yourself and your family • Understand the privacy settings and defaults • Consider who you accept as a friend online carefully • Create strong passwords and user names • Beware of links to games, quizzes, advertising, and other applications available through social networking sites
If you encounter classified or other official documents not authorized for public release on the internet, follow Best Practices	• Do not download it • Report it to your security POC